Domain - Technology - Core Services - EC2

Amazon EC2

About Amazon EC2

01 This is scalable compute capacity provided on Amazon Web Services.

02 Here AWS takes care of the underlying physical infrastructure. You don’t need to invest in hardware.

03 You can create an EC2 Instance and terminate the instance when it is not required.

About VPC

01 When you deploy an EC2 Instance it needs to be part of a virtual network on the cloud.

02 This virtual network in AWS is known as a Virtual private cloud.

03 Within a VPC, you also have subnets. This is a range of IP addresses in the VPC.

Instance Connect

EC2

Instance Connect - Amazon EC2

01 Provides a simple and secure way to connect to Linux instances.

02 You can also control the access to the connecting to the instance via IAM policies.

03 You need to install the EC2 Instance Connect on the instance.

Instance State

pending

This is the state when the instance is first being launched. You are not billed here.

running

Here the instance is in the running state. You are billed for the instance.

stopped

Here the instance is shut down. You are not billed for the instance

terminated

Here the instance is completely deleted.

EC2 Instance Types

Instance Types

General Purpose

These instances provide a balance of compute, memory and network resources.

This is ideal for general purpose workloads like hosting web servers.

Compute Optimized

This is ideal for applications that need a lot of high performance when it comes to CPU. Gaming servers, machine learning applications, high performance web servers.

Memory Optimized

This is ideal for applications that process large amounts of data in memory.

In-memory caches, Hadoop and Spark clusters.

Instance Types

Accelerated Computing

Here the application could need to make use of hardware accelerators.

Sometimes gaming applications require these capabilities.

Storage Optimized

This is ideal for hosting database servers that require high, sequential read and write access to large data sets.

Summary Points

About VPC

01 This is an isolated network on the AWS Cloud.

02 All VPC’s are isolated from one another.

03 A VPC is launched in a region. It also has a CIDR block configured.

Default VPC

01 This is created in each region.

02 A default subnet is created in the VPC. A subnet is created for each Availability Zone.

03 An Internet gateway is created and connected to the default VPC.

Default VPC

04 There is a main route table that points all Internet traffic to pass via the Internet gateway.

05 There is a default security group associated with the default VPC.

06 There is a default network access control list associated with the default VPC.

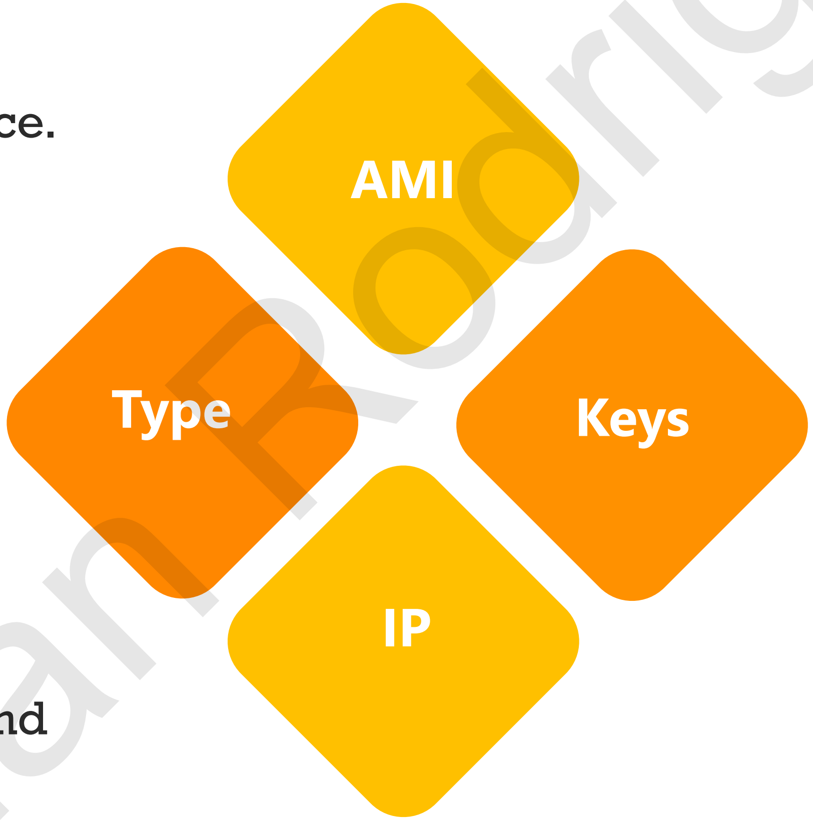
Other Aspects

Amazon Machine Image

The image has the required information to launch the instance.

Instance type

This is a combination of CPU, Memory, Storage, Networking and other capabilities.



Key Pair

This is a combination of a public and private key. The public key is stored on your Linux-based instance. You use the private key to securely SSH into the instance.

Public IP

This allows your instance to be reachable from the Internet.

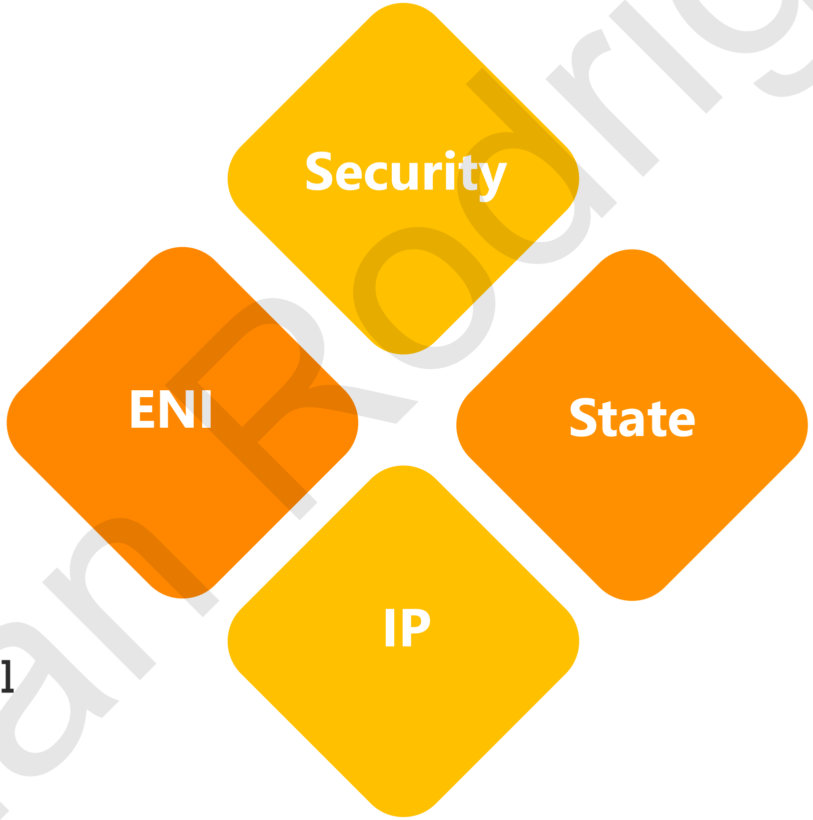
Other Aspects

Security Group

This controls the traffic that is inbound and outbound from a resource. Rules are present to control the traffic.

Instance state

We can change the instance state at any point in time – We can stop and terminate the instance.



Elastic Network Interface

This is used to represent a virtual network card.

Workloads

We can setup workloads on the instances.

AWS Region

01 This is a physical location in the world where AWS has their data centers.

02 For certain services we need to choose a particular region.

03 AWS keeps on expanding the number of regions.

AWS Availability Zones

01 This is one or more discrete data centers with redundant power, networking and connectivity.

02 Each AWS region has a number of Availability Zones.

03 All Availability zones are interconnected with high-bandwidth, low-latency networking.

AWS Dedicated Hosts

01 This is a physical server that is fully dedicated to you.

02 You can create EC2 Instances on the dedicated host.

03 This is ideal to use when you have per-VM software licenses or per-core licenses.

Amazon EC2 Pricing

01 The pricing defers from region to region.

02 It also depends on the Instance type and operating system you use.

03 But you can only pay for how much you use – This is where you get so much flexibility when it comes to the pricing.

Domain - Technology - Core Services - Storage

Amazon Elastic File System

Summary Points

Amazon EBS Volumes

01 EBS – Elastic Block Storage.

02 This is durable, block-level storage devices that can be attached to instances.

03 The EBS volumes can be mounted as devices on the instances.

Amazon EBS Volumes

01 You can attach multiple volumes to an EC2 Instance.

02 The volume and instance must be in the same Availability Zone.

03 You can also attach one volume to multiple instances.

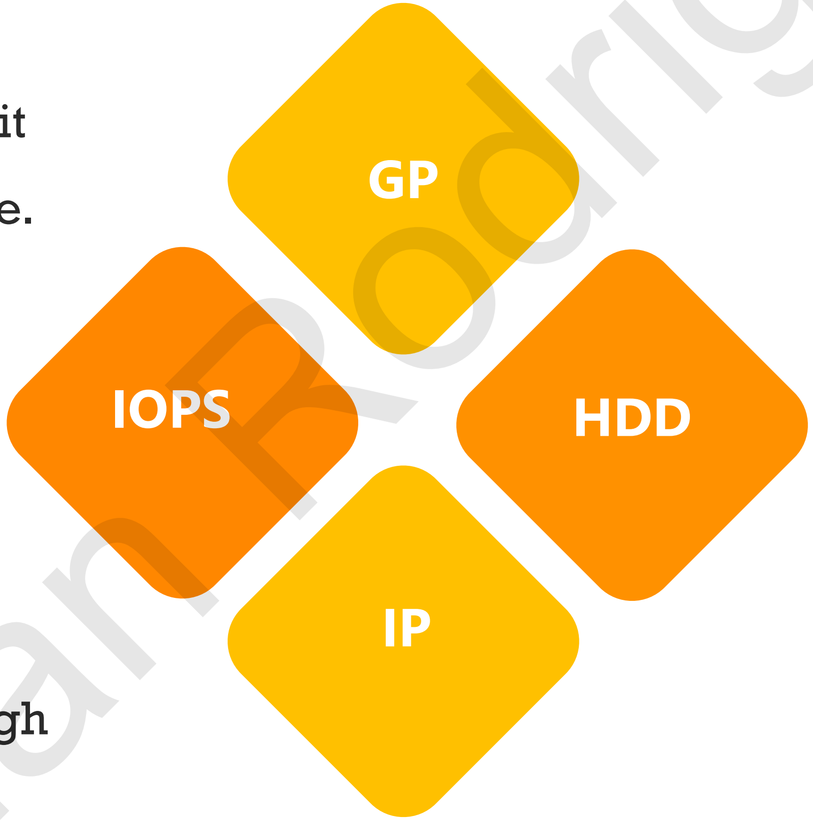
Volume Types

General Purpose SSD(gp2, gp3)

These are backed by solid-state drives. Provide a balance when it comes to price and performance.

Provisioned IOPS (io1, io2)

These are also backed by solid-state drives. But they provide high performance. Great for critical workloads.



Throughput Optimized HDD

Good for workloads that depends on getting good throughput , frequently accessed data – Data warehousing applications.

Cold HDD

This is good for workloads that are not accessed that frequently.

Amazon EBS Snapshots

01 These are point-in-time snapshots of the Amazon EBS Volumes.

02 The snaphots taken are incremental in nature.

03 You can restore the snapshot to an EBS volume.

EC2 Instance Store

01 This is temporary block-level storage for the instance.

02 The storage is located on the disks that are physically attached to the host computer.

03 This is great when you want to store a lot of local data like buffer data.

Amazon Elastic File System

01 This allows you to create a file system in AWS.

02 Here the underlying storage is completely managed for you.

03 Multiple resources like Amazon EC2, AWS Lambda can then connect to the file system.

Amazon Elastic File System

01 If you want locally assigned storage for just an EC2 Instance – Make use of EBS volumes.

02 If you want a file system that needs to be shared across multiple EC2 Instances – Elastic File System.

Summary Points

Amazon EBS Volumes

01 EBS – Elastic Block Storage.

02 This is durable, block-level storage devices that can be attached to instances.

03 The EBS volumes can be mounted as devices on the instances.

Amazon EBS Volumes

01 You can attach multiple volumes to an EC2 Instance.

02 The volume and instance must be in the same Availability Zone.

03 You can also attach one volume to multiple instances.

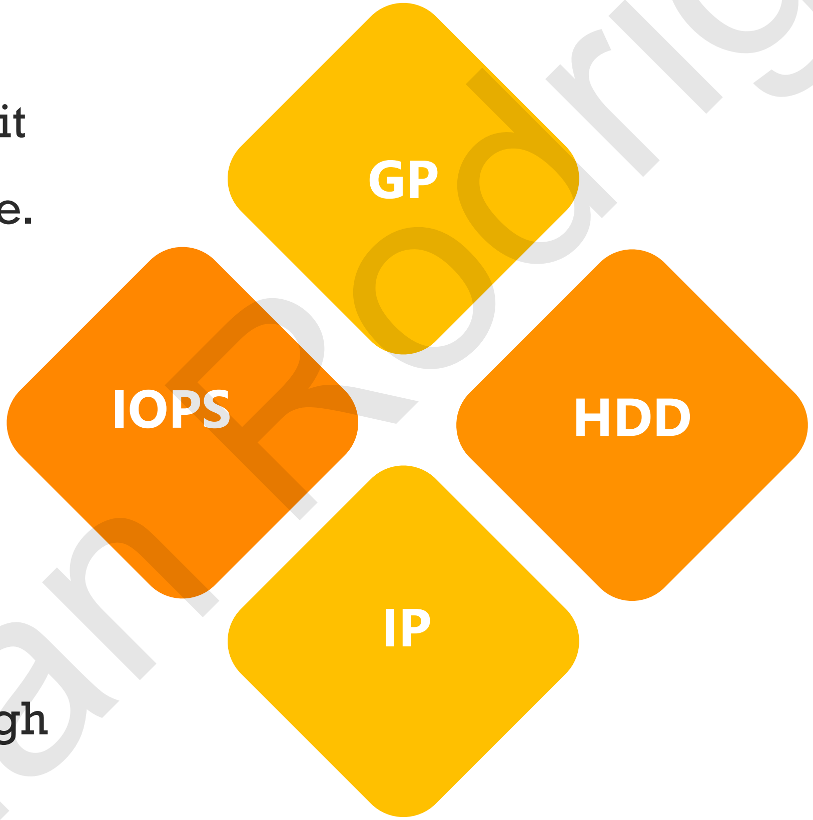
Volume Types

General Purpose SSD(gp2, gp3)

These are backed by solid-state drives. Provide a balance when it comes to price and performance.

Throughput Optimized HDD

Good for workloads that depends on getting good throughput , frequently accessed data – Data warehousing applications.



Provisioned IOPS (io1, io2)

These are also backed by solid-state drives. But they provide high performance. Great for critical workloads.

Cold HDD

This is good for workloads that are not accessed that frequently.

Amazon EBS Snapshots

01 These are point-in-time snapshots of the Amazon EBS Volumes.

02 The snaphots taken are incremental in nature.

03 You can restore the snapshot to an EBS volume.

EC2 Instance Store

01 This is temporary block-level storage for the instance.

02 The storage is located on the disks that are physically attached to the host computer.

03 This is great when you want to store a lot of local data like buffer data.

Storage Classes

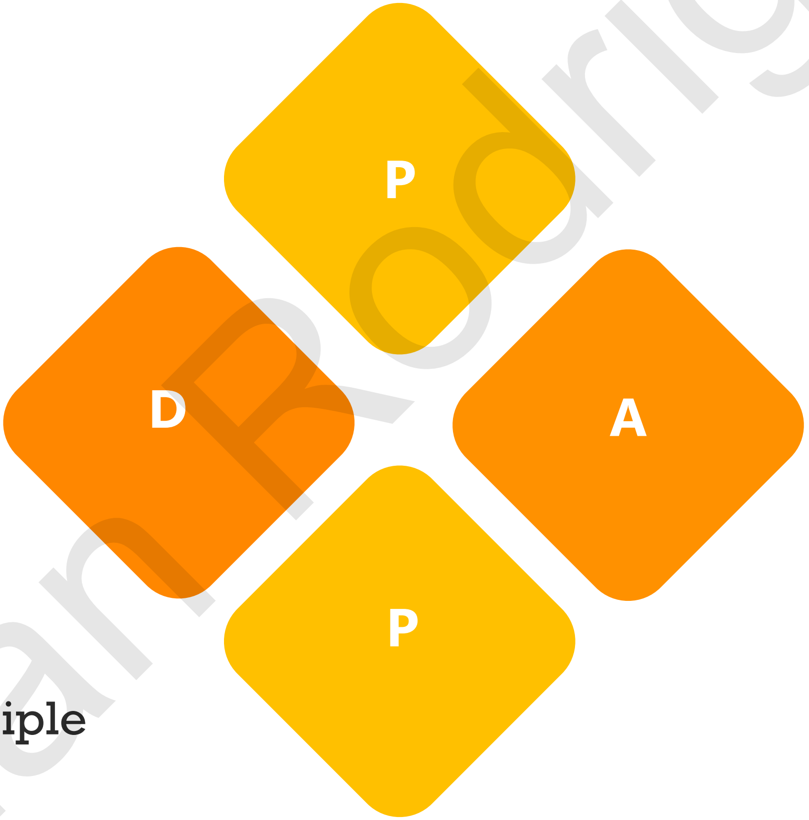
S3 Standard

Performance

Provides low latency and high throughput performance.

Availability

Designed for 99.99% availability.



Durability

Designed for 99.999999999% durability of objects across multiple Availability Zones.

Purpose

Can be used for common use cases when it comes to storage of data.

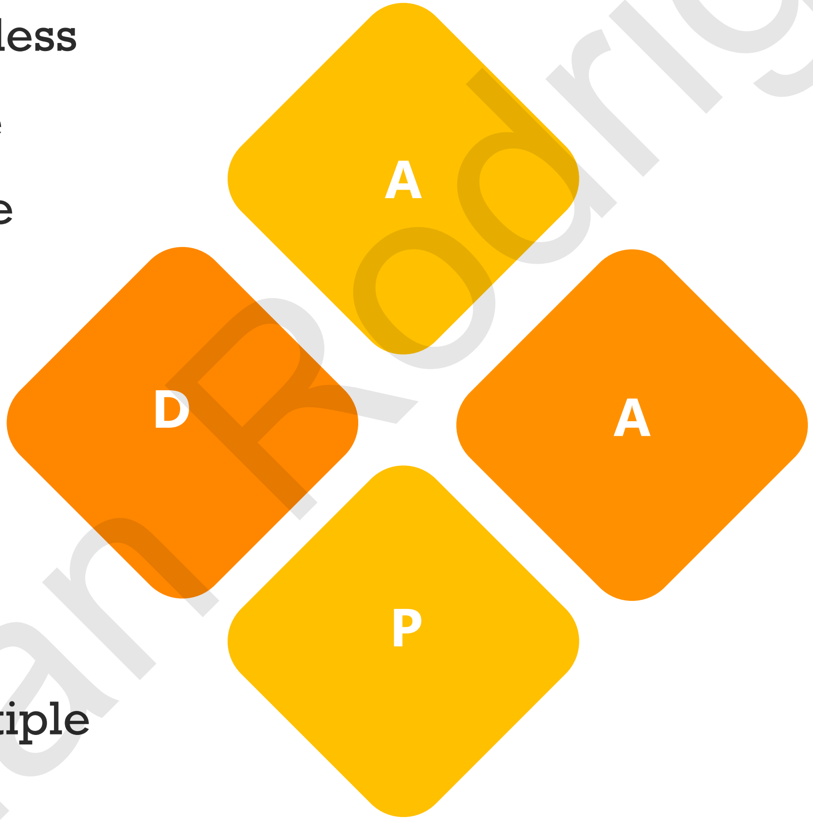
S3 Standard-IA

Access

This is for data that is accessed less frequently. You get a lower price when it comes to per GB storage and per GB retrieval.

Availability

Designed for 99.9% availability.



Durability

Designed for 99.999999999% durability of objects across multiple Availability Zones.

Purpose

Ideal for backup of data.

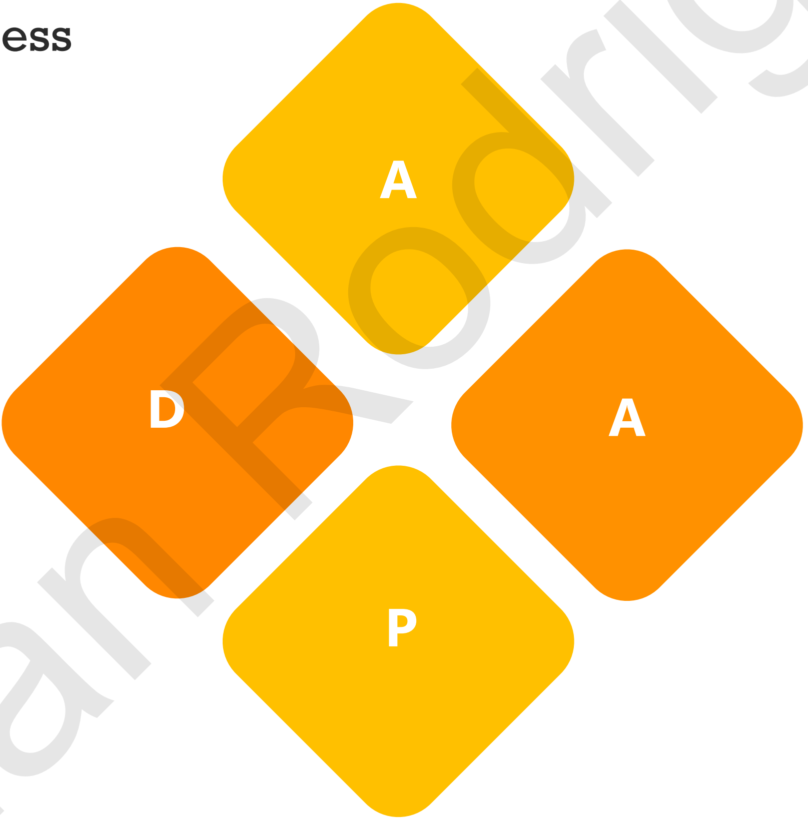
S3 One Zone-IA

Access

This is for data that is accessed less frequently. But when you want to access the data, you need it immediately.

Availability

Designed for 99.5% availability.



Durability

Designed for 99.999999999% durability of objects in a single Availability Zone.

Purpose

You want a low-cost option for storing data and don't mind the less resiliency when it comes to data storage.

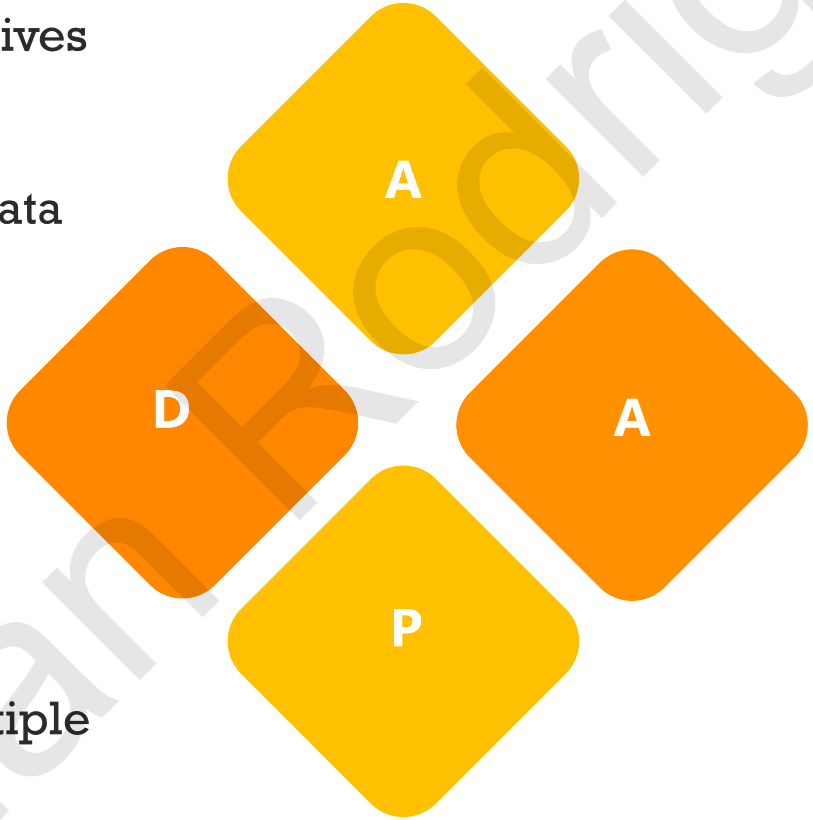
S3 Glacier Instant Retrieval

Access

This is an archive solution that gives low-cost storage. This can be chosen if you want retrieval of data in milliseconds.

Durability

Designed for 99.999999999% durability of objects across multiple Availability Zone.



Availability

Designed for 99.9% availability.

Purpose

Archive data that requires immediate access.

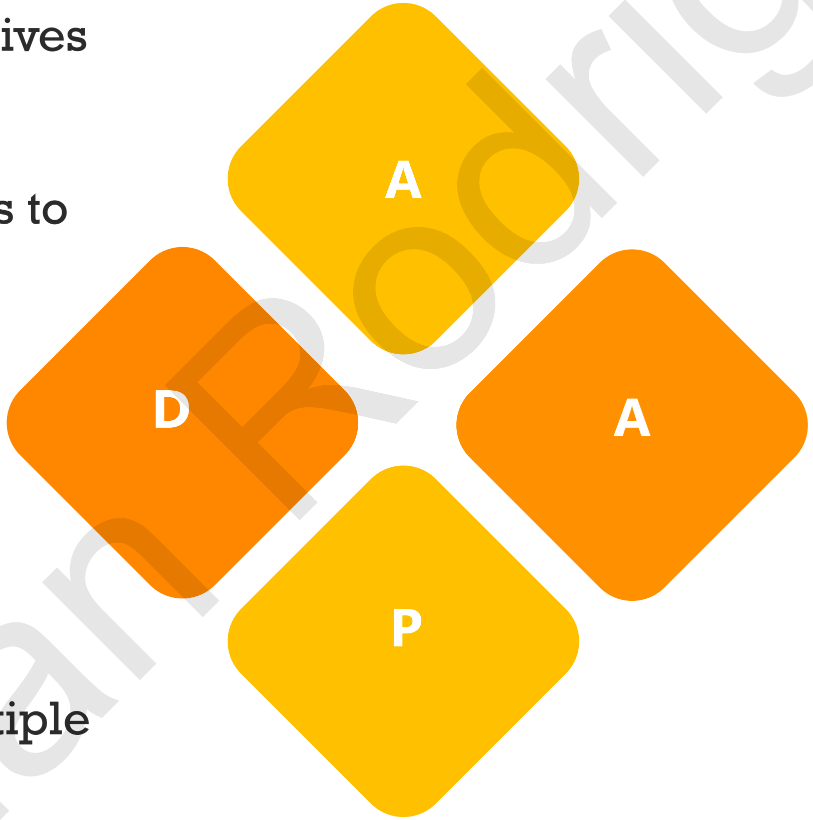
S3 Glacier Flexible Retrieval

Access

This is an archive solution that gives low-cost storage. Here the data retrieval can range from minutes to hours.

Availability

Designed for 99.99% availability.



Durability

Designed for 99.999999999% durability of objects across multiple Availability Zone.

Purpose

Archive data that needs to be accessed very rarely.

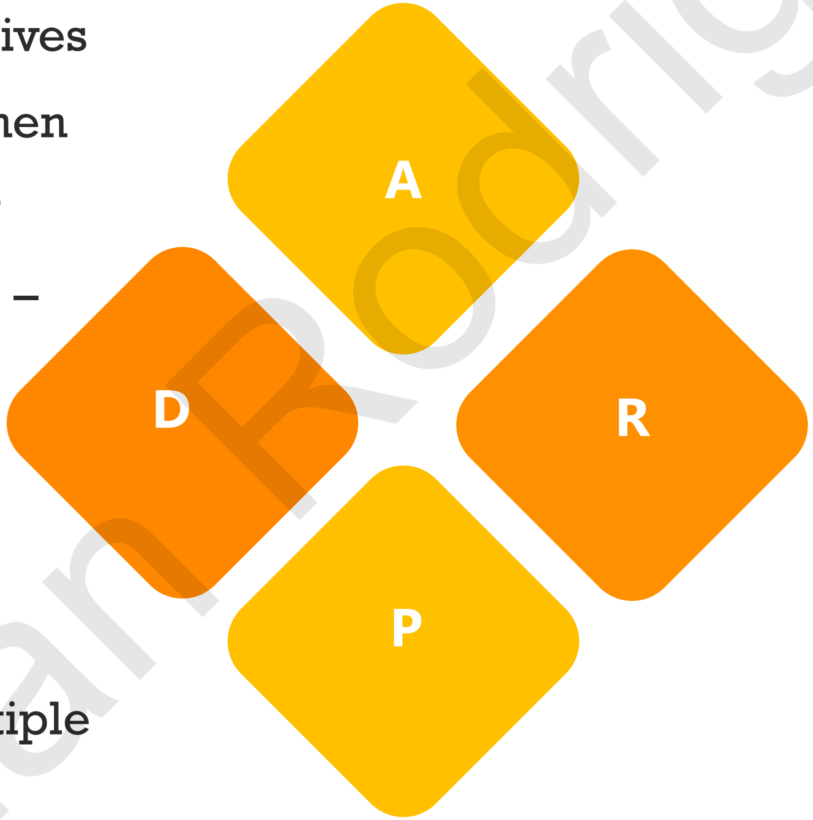
S3 Glacier Deep Dive

Access

This is an archive solution that gives low-cost storage. This is used when organizations want to store their data for long periods of time – 7 – 10 years.

Durability

Designed for 99.999999999% durability of objects across multiple Availability Zone.



Retrieval

Here the retrieval time can be within 12 hours.

Purpose

Could be used as an alternative when organizations use magnetic tapes for backup purposes.

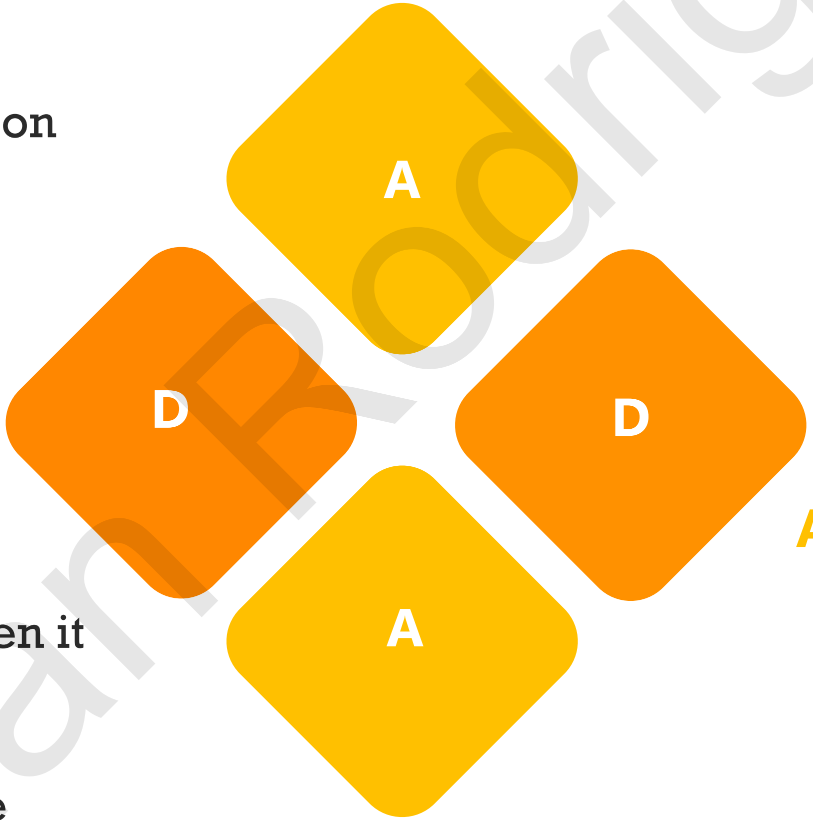
S3 Intelligent-Tiering

Access

This feature moves data to most cost-effective access tier based on the access of data.

Durability

Designed for 99.999999999% durability across multiple Availability zones.



Charge

Here there is a small charge when it comes to monitoring data to understand the tier to set for the object.

Availability

Designed for 99.9% availability.

S3
Transfer Acceleration

S3 Transfer Acceleration

01 This is a bucket-level feature available with Amazon S3.

02 This enables fast and secure transfer of files over long distances.

03 These are the file transfers that occur between the client and the S3 bucket.

S3 Transfer Acceleration

01 The transfer acceleration feature makes use of the distributed edge locations when it comes to Amazon CloudFront.

02 You must enable this feature for a bucket.

03 There is a different bucket URL that can be used when making use of the transfer acceleration feature.

Amazon RDS

Amazon RDS

01 This is the Amazon Relational Database service.

02 This service makes it easier to setup a database on the AWS Cloud.

03 The supported database engines – MySQL, Oracle , Microsoft SQL Server, PostgreSQL and MariaDB.

Amazon RDS

01 There is high availability built into the service.

02 It manages backups, software patching , failure detection etc.

03 The entire infrastructure is managed by AWS.

Amazon Aurora

Amazon Aurora

01 This is a fully managed relational database engine that is compatible with MySQL and PostgreSQL

02 Amazon Aurora can deliver more throughput when compared with MySQL and PostgreSQL.

03 Here again the underlying infrastructure is completely managed for you.

Amazon DocumentDB

Amazon DocumentDB

01 This is a fully-managed database service.

02 This is used when you want to setup MongoDB-compatible databases on the cloud.

03 This is a document-based database.

Amazon DocumentDB

01 Here the data can be stored as JSON documents.

02 With Amazon DocumentDB, the storage grows as the need to store data grows.

03 You can also scale compute and memory resources as required.

Amazon EMR

Amazon EMR

01 This service is known as Amazon Elastic MapReduce.

02 Here you can run your big data workloads using Apache Hadoop and Apache Spark.

03 This service can be used to process and analyze large amounts of data.

Amazon EMR

01 Via the use of this service, you provision a cluster of nodes.

02 You can then submit jobs that need to process data to the cluster.

Amazon Neptune

Amazon Neptune

01 This is a fully-managed graph database service.

02 This is a highly available service and all of the data is backed-up to Amazon S3.

03 Graph databases - Data items and relationships between data items.

Amazon Neptune

01 For example, if you want to store the company employee hierarchy, you can make use of a graph database.

02 The data items are stored as vertices of a graph.

03 The relationships are stored as edges.

Amazon QuickSight

Amazon QuickSight

01 This is a cloud-based business intelligence service.

02 You can use this service to connect to various data sources on the cloud.

03 You can then visualize the data from the various sources.

Amazon Redshift

Amazon Redshift

01 This is a fully managed, petabyte-scale data warehouse service in AWS.

02 This is normally used for hosting your data warehouses.

03 You can get a cluster of nodes for hosting your data.

Amazon Athena

Amazon Athena

01 This is an interactive query service.

02 It allows you to analyze data that is stored in Amazon S3 via the use of Standard SQL queries.

03 Here you don’t pay for any infrastructure. You only pay for the queries run.

AWS Global Accelerator

AWS Global Accelerator

01 This is used to create accelerators that can be used to improve the performance of your applications for local and global users.

02 Standard Accelerators – These can direct traffic via the use of the AWS Global network to the endpoints in the region that is closest to the user.

03 With the Global accelerator , you get static IP addresses that need to be associated with the accelerator.

AWS Global Accelerator

01 Standard accelerators – Here the endpoints are Network Load Balancers, Application Load Balancers , Amazon EC2 Instances, Elastic IP addresses.

02 Custom routing accelerators – Here the endpoints are virtual private cloud subnets which has EC2 Instances.

AWS
Storage Gateway

AWS Storage Gateway

01 This service can be used to extend the on-premises storage requirement to the cloud.

02 This can help reduce costs for the company, since they don’t need to invest on capital costs for buying new storage devices.

03 **Amazon S3 File Gateway** – Here the data is stored on S3. The objects stored in S3 are made available as files to the on-premises client.

AWS Storage Gateway

01 **Amazon FSx File Gateway** – Here the file data is stored in Amazon FSx and has Windows native compatibility for Access Control Lists and Shadow copies.

02 **Tape Gateway** – Here you can store your virtual tapes in Amazon S3.

03 **Volume Gateway** – Here block storage volumes are available using the iSCSI protocol.

Domain - Technology - Services

AWS Trusted Advisor

AWS Trusted Advisor

01 This provides recommendations based on which you can follow AWS best practices.

02 The basic checks are only available as part of AWS Basic and AWS Developer Support.

03 For all checks, you need to upgrade to AWS Business or Enterprise Support.

AWS Trusted Advisor

Cost Optimization

The tool can help identify ways to save on costs – underutilized EBS volumes, unassociated Elastic IP addresses

Performance

You get recommendations on how to improve the performance of your environment – Compute usage of EC2 Instances.

Security

You get recommendations on how to improve the security of your environment – Security Group risks.

AWS Trusted Advisor

Fault tolerance

The tool can help identify ways to improve the reliability of your environment.

Service quotas

You can see how the resources you are creating are compared against the account quotas.

AWS
Connectivity

AWS VPN

01 This can be used to setup a connection between your on-premises network and an AWS VPC.

02 Here the connection is encrypted and secure.

03 This service is highly available.

AWS Direct Connect

01 This provides a direct link between the on-premises network and AWS.

02 Here there is a connection to an AWS Direct Connection Location over the standard Ethernet fibre-optic cable.

03 You can create connections to your AWS VPC and AWS Public services as well.

AWS Lambda

AWS Lambda

01 This a compute service that allows you to run code on the cloud without the need of provisioning servers.

02 AWS Lambda manages the entire infrastructure for you.

03 You only pay for the amount of compute you use.

Amazon Lightsail

AWS Lightsail

01 This is a virtual private server provider.

02 This is another compute option that allows you to host applications on the cloud.

03 Lightsail has everything included to jumpstart your solution – EC2 Instances, databases , DNS Management etc.

Amazon SQS

Amazon SQS

01 This is the Simple Queue service.

02 This provides a secure, durable and fully managed queue service.

03 It can be used to decouple distributed software systems and application components.

Amazon SNS

Amazon SNS

01 This is the Simple Notification service.

02 This service provides message delivery from publishers to subscribers.

03 The publishers can send messages to a topic.

Amazon SNS

01 Subscribers can subscribe to a topic and receive the messages.

02 Consumers be mobile devices for mobile push notifications or text messages.

03 Consumers can also be AWS services like Amazon SQS, AWS Lambda etc.

Amazon MQ

01 This is a managed message broker.

02 If a company is already using a messaging broker system like Apache ActiveMQ or RabbitMQ, they can consider migrating to the Amazon MQ service.

03 It has support for a variety of protocols such AMQP 0-9-1, AMQP 1.0, MQTT, OpenWire, and STOMP.

Amazon
EC2 Auto Scaling

Amazon EC2 Auto Scaling

01 This services ensures you have the right number of EC2 Instances running at a time.

02 Your EC2 Instances are created as part of Auto Scaling groups.

03 You can define the minimum number of instances that need to run as part of the group.

Amazon EC2 Auto Scaling

01 You can also define the maximum number of instances that need to run as part of the group.

02 You can define scaling policies that determine when the instances should be created or terminated.

03 Benefits of using this service – **Better fault tolerance, Better availability and Better cost management.**

AWS CloudFormation

AWS CloudFormation

01 This is a service that can deploy your AWS resources based on a template definition.

02 The template can be in JSON or YAML format.

03 CloudFormation creates a stack of resources based on the template definition.

AWS Beanstalk

AWS Beanstalk

01 You can use this service to quickly deploy applications to the AWS Cloud without the need of understanding the infrastructure aspects.

02 This service will create the environment for you.

03 You can then upload your application to the environment.

AWS Beanstalk

01 This service has support for applications developed in Go, Java, .NET,. Node.js, PHP, Python and Ruby.

02 This service will create the EC2 Instances that can be used for hosting the environment.

03 This service also manages aspects such as capacity provisioning, load balancing, scaling and application health monitoring.

AWS
OpsWorks

AWS OpsWorks

01 This is a configuration management service.

02 You can manage the configuration of your applications by using tools such as Puppet or Chef.

03 OpsWorks can manage the different aspects of your application deployment via the use of stacks.

AWS OpsWorks

01 **Stack** – This is a container of resources such as Amazon EC2 Instances, Amazon RDS databases etc.

02 **Layers** – You can split the different application components running as part of your stack in different layers.

03 **Chef** – You can use the Chef tool to manage the different layers of the stack.

AWS

Batch

AWS Batch

01 This service allows you to run batch computing workloads in AWS.

02 Here AWS will automatically manage the compute resources and optimize the workload distribution.

03 Jobs are created based on job definitions. And the jobs are submitted to the compute instances.

Amazon Kinesis

Amazon Kinesis

01 This service is used to ingest data at scale.

02 This is the fully managed service, you don’t need to worry about the infrastructure.

03 Used to collect , process and analyze real-time and streaming data.

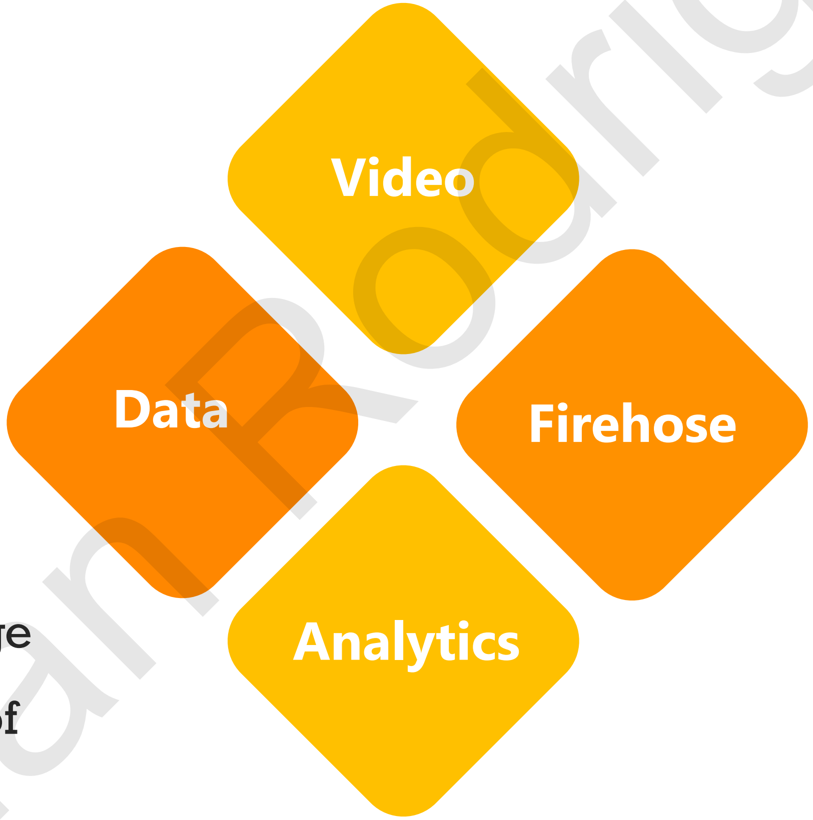
Amazon Kinesis

Kinesis Video Streams

This service allows to securely stream video from connected devices to AWS.

Kinesis Data Firehose

This service can be used to capture, transform and load data streams into AWS data stores for real-time analytics.



Kinesis Data Streams

This can be used to capture large amounts of data from a variety of data sources.

Kinesis Data Analytics

This service can be used to process data streams in real time with SQL or Apache Flink.

Amazon Connect

Amazon Connect

01 This is a cloud-based contact center.

02 You can actually create personalized experiences for customers.

03 Agents also have an easy way to deal with customers.

Amazon Connect

01 **Getting started** – Create an instance of Amazon Connect.

02 Set up the required phone numbers for the contact center.

03 You can then create queues, create a flow on how the customer experience would be implemented.

Amazon API Gateway

Amazon API Gateway

01 This is used for creating, publishing, maintaining, monitoring and securing REST, HTTP and WebSocket APIs at scale.

02 You can implement the standard HTTP methods of GET, POST, PUT, PATCH and DELETE.

03 You make the API Gateway as the entry point for requests for your users.

Amazon API Gateway

01 You could have your workloads running on backend services such as Amazon EC2 Instances or AWS Lambda.

02 You can combine this service with AWS IAM for authentication.

03 If you are making use of HTTP API's, you can also make use of Open ID Connect and OAuth 2.0 for authorization.

Amazon Workspaces

Amazon Workspaces

01 This service allows you to provision cloud-based Microsoft Windows or Amazon Linux desktops for users.

02 Here you create something known as Workspaces.

03 With the workspace you can start provisioning the machines.

Amazon Workspaces

01 You can deploy applications via the use of Amazon Workspaces Application Manager.

02 For Windows-based desktops you can bring your own licenses and applications.

03 Remember that you are still responsible for patching the machines in the workspace.

Amazon AppStream

Amazon AppStream

01 This is a fully managed application streaming service.

02 You can provide users with instant access to applications from anywhere.

03 AppStream will manage the resources that are needed to run the applications.

Amazon AppStream

01 The user can run the application on the device of their choice.

02 You can use the AppStream client to access the application.

AWS

Transit Gateway

AWS Transit Gateway

01 This is a network transit hub that can be used to interconnect virtual private clouds and on-premises networks.

02 You can attach one or more VPC's in different regions.

03 If you have an AWS Direct Connect gateway, this can also be used with the transit gateway.

AWS
Load Balancer

Network Load Balancer

01 This load balancer works at the Network Layer.

02 You can use this Load Balancer to distribute requests to targets such as Amazon EC2 Instances.

03 The Load Balancer automatically scales based on demand.

Application Load Balancer

01 This load balancer works at the Application Layer.

02 You can route requests based on the URL in the request.

03 You can route requests based on the HTTP headers values in the request.

Gateway Load Balancer

01 This service enables you to deploy and manage virtual appliances such as firewalls, intrusion detection systems.

02 This load balancer works at the network layer.

03 It listens for the IP packets and then forwards the traffic to the appropriate target group.

Amazon
Route 53

Amazon Route 53

01 This is a highly available and scalable Domain Name System.

02 Here you can register your domain names.

03 You can route internet traffic to your domain.

Amazon Route 53

01 You can create a hosted zone. This zone contains records.

02 Public hosted zone – This specifies how to route traffic on the internet.

03 The records has information on how traffic needs to be routed.

Amazon Route 53

01 **Simple routing policy** – This can be used to direct traffic to a single resource.

02 **Failover routing policy** – This can be used to direct traffic to a secondary site if the primary one goes down.

03 **Latency routing policy** – This can direct the users request to the closest region, the response that would give the least latency.

Amazon CloudFront

AWS CloudFront

01 This service can be used to speed up the distribution of static and dynamic content.

02 Here requests are routed via edge locations that provide the least latency.

03 Here the content is routed via the AWS backbone network to the edge location to route the request faster to the user.

Amazon Rekognition

Amazon Rekognition

01 This is a recognition service.

02 You can submit videos and images to the service for analysis.

03 It can then detect objects such as people, text, scenes.

Amazon Rekognition

01 It can also detect inappropriate content.

02 You can detect , analyze and compare faces.

Amazon Transcribe

Amazon Transcribe

01 This is an automatic speech recognition service.

02 It is used to covert audio to text.

03 It uses machine learning models to achieve this.

Amazon Polly

Amazon Polly

01 This service is used to convert text to speech.

02 There are different voices available in different languages.

03 You can build applications that can embed the use of this service.

Amazon Translate

Amazon Translate

01 This service is used to translate text from one language to another.

02 Here it can automatically detect the language in the source text.

03 It uses machine learning to translate the text.

Amazon Comprehend

Amazon Comprehend

01 This service is used to Extract insights from documents.

02 It can detect entities , key phrases based on the context in the documents.

03 It makes use of a pre-trained model to gain insights about the content stored in the document.

AWS

Application Discovery Service

AWS Application Discovery service

01 This service can help in the migration process of your on-premises environment to the cloud.

02 It collects the usage and configuration data about the on-premises servers.

03 You can see the servers , see their utilization.

AWS
Backup

AWS Backup

01 This is a fully managed service that provides data protection.

02 Here you can create backup policies, automate backup schedules.

03 You can specify how often the backups should be taken and for how long to retain the backups.

AWS Backup

01 You can use this service for Amazon EC2.

02 Here AWS Backup will protect the Amazon EBS volumes attached to the instance.

AWS
Migration

AWS Server Migration Service

01 This helps to automate the migration of on-premises VMware vSphere, Microsoft Hyper-V machines to the AWS Cloud.

02 Here the server VM's are replicated to Amazon Machine Images.

03 Whenever the images are ready, they can be deployed as EC2 Instances.

AWS Database Migration Service

01 This services makes it easier to migrate relational databases, data warehouses and other types of data stores to the cloud.

02 You can perform a one-time migration or even replicate on-going changes from the source to the target.

03 You can also migrate to a different database engine with the help of the AWS Schema Conversion tool.

Domain – Security and Compliance

Identity and Access Management

AWS IAM

01 This is AWS Identity and Access Management.

02 This is a web service that allows you to securely control access to AWS Resources.

03 You can define identities and then give permissions to those identities.

AWS IAM Key Terms

Principal

This is a person or application that makes a request for an action or an operation that needs to be performed on an AWS resource.

Authentication

Normally a user needs to be authenticated first to AWS before they can make resource requests.

Authorized

Once authenticate, AWS will check to see if you are authorized, basically have the required permissions to access a resource.

AWS IAM root user

01 By default, when you create an AWS account, a user gets created which is the root user.

02 This root user has access to all resources in the AWS account.

03 Never use the root user to perform day-to-day operations.

AWS IAM Users

01 You can create an IAM user. This user is part of your account.

02 The user can be allocated a password that can be used to log into the AWS account.

03 The user can also get access keys that can be used for programmatic access to the AWS account.

AWS IAM Policies

01 IAM policies are used to grant permissions to users.

02 A policy is just an object that can associated with an identity or a resource.

03 Based on the policy a user could be granted or denied access to a resource.

IAM Security

Best practices

AWS IAM Best practices

01 Require the use of Multi-Factor Authentication.

02 Rotate access keys for long-term access credentials.

03 Protect your root user credentials.

AWS IAM Best practices

01 Apply least-privilege permissions wherever possible.

02 Perform a regular review of users, roles, permissions, policies etc.

03 Verify the public access you might have provided in the AWS account.

Amazon Macie

Amazon Macie

01 This is a fully managed data security and data privacy service.

02 It uses machine learning to help discover, monitor and protect sensitive data in your AWS environment.

03 It Analyses the data in your S3 buckets.

Amazon Macie

01 It provides an inventory for your S3 bucket.

02 It creates detailed findings that you can remediate as required.

IAM User

Access keys

IAM User Access keys

01 These are long-term credentials for an IAM user.

02 You can use the access keys when it comes to programmatic requests made to AWS.

03 Access keys consists of two parts.

IAM User Access keys

01 Access key ID and the secret access key.

02 Both must be specified when making the programmatic request.

Secrets Manager

AWS Secrets Manager

01 This service allows you to store secrets. Applications can then make a secure call to the AWS Secrets Manager to get the value of the secret.

02 You can also make AWS Secrets Manager rotate the value of a secret.

03 This is a completely managed service.

AWS Secrets Manager

01 A secret consists of secret information, the secret value and metadata about the secret.

02 The secret value can be a string or binary.

03 An encryption key from the AWS Key Management service is used to encrypt and decrypt the secret value.

AWS

Security Groups

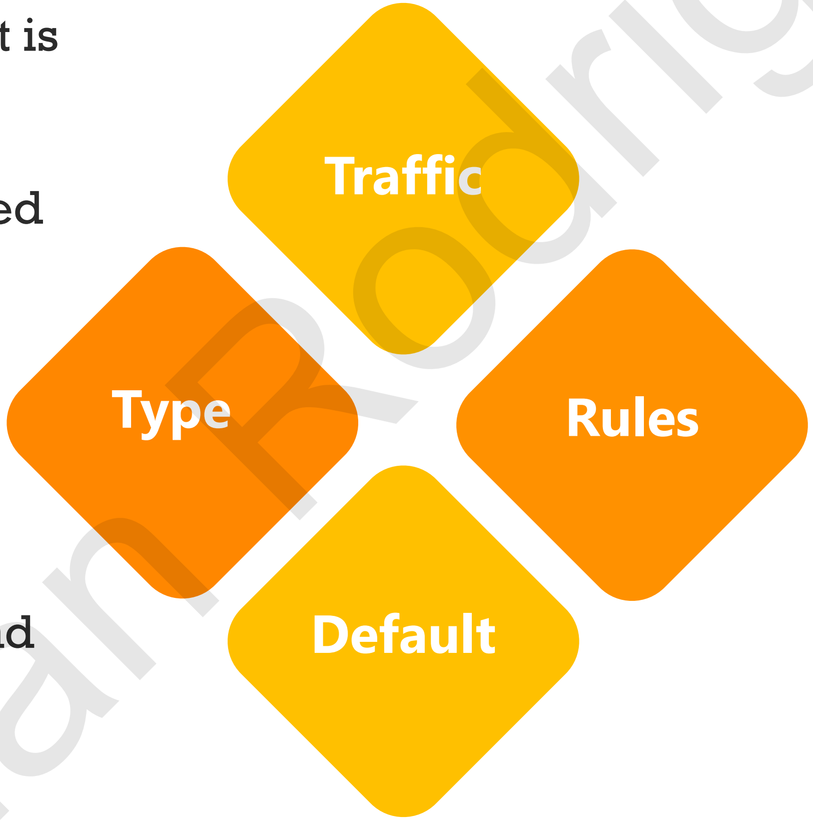
AWS Security Groups

Control traffic

This is used to control traffic that is allowed to reach and leave resources that they are associated with.

Traffic type

Here you can control the Inbound and Outbound traffic.



Rules

In the Security Group, you define rules that control traffic based on protocols and port numbers.

Default

The default VPC and any VPC you create comes with a default security group.

Network

ACL

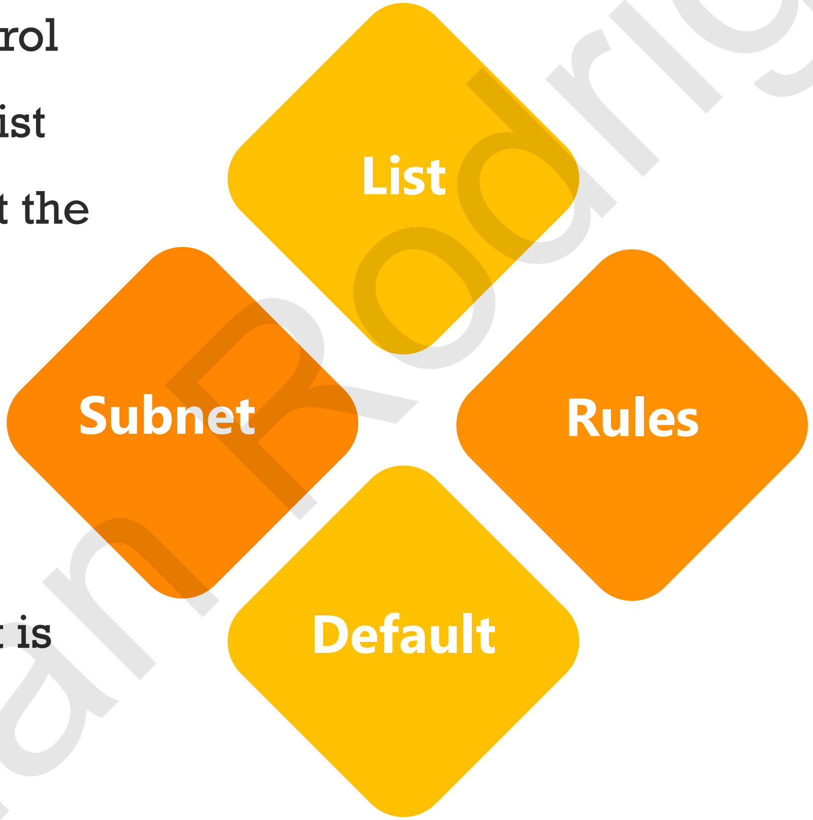
Network ACL

List

These are Network Access Control Lists. A network access control list is used to allow or deny traffic at the subnet level.

Rules

Here again you can define Inbound and Outbound rules.



Subnet

The Network Access Control list is attached to a subnet.

Default

The default VPC comes with a default NACL.

Amazon
Detective

Amazon Detective

01 This service can be used to analyze and investigate the root cause of any security findings or suspicious activities.

02 This service collects log data from your AWS resources.

03 It then uses machine learning to analyze the data and come up with its own security findings.

AWS

Key Management Service

AWS Key Management Service

01 This service is used to manage your cryptographic keys.

02 This service uses hardware security modules to protect and validate the keys.

03 It also integrates with other services on AWS.

AWS Key Management Service

01 You can create both symmetric and asymmetric keys.

02 You can control access to the keys via the use of key policies, IAM policies.

03 You can also enable the rotation of keys.

Amazon Inspector

Amazon Inspector

01 This is a vulnerability management service.

02 You can use this service to scan for vulnerabilities in your Amazon EC2 Instances and container images that reside in Amazon Elastic Container Registry.

03 The service then creates findings based on the vulnerabilities that are discovered.

Amazon Inspector

01 It can identify software packages that are exposed to common vulnerabilities.

02 It also analyses the network paths to your EC2 Instances.

Amazon CloudWatch

Amazon CloudWatch

01 This is used to monitor your AWS resources in real-time.

02 You can also create dashboards to display the graphs for various metrics.

03 You can also define alarms that can be used to perform an action if a particular threshold has been reached.

Amazon CloudWatch Logs

Amazon CloudWatch Logs

01 This is a central repository for storage of logs.

02 You can stream your logs from sources like your EC2 Instances.

03 You can then analyze the logs collected via the use of executing queries against the collected data.

AWS
CloudTrail

AWS CloudTrail

01 This service is used from an auditing and governance perspective.

02 Here all of the actions taken by a user, role or an AWS service are recorded as events in AWS CloudTrail.

03 With the help of CloudTrail logs you can identify any sort of suspicious or unusual activity in your AWS account.

AWS CloudTrail

01 By default, AWS CloudTrail is already enabled for an account.

02 You can view the events from the last 90 days for your account.

03 If you want to maintain your logs for a longer time, you can deliver the events to an Amazon S3 bucket.

AWS

Health Dashboard

AWS Health Dashboard

01 Here you can see any sort of events that could have an impact on your account.

02 You can see also see any scheduled maintenance activities that would be performed by AWS that could affect your account.

03 You can use the Event log to view all of the AWS Health events.

Amazon EventBridge

Amazon EventBridge

01 This service can be used to deliver a stream of real-time data from applications or AWS services to targets such as AWS Lambda.

02 EventBridge has the capability to receive an event, apply a rule and then route the event to a target.

03 You can archive events and replay them at a later point in time.

AWS
Config

AWS Config

01 This service can first be used to discover supported resources in an AWS account.

02 It can also detect configuration changes for a resource.

03 It maintains historical records of the configuration items of resources.

AWS Config

01 AWS Config can be used to send the updated configuration changes to an Amazon S3 bucket.

02 You can have rules that trigger AWS Lambda functions when configuration changes occur.

AWS

Systems Manager

AWS Systems Manager

01 This service allows you to manage the applications and infrastructure running in AWS.

02 **Application Manager** – This allows teams to investigate issues with their AWS resources in the context of applications that are running on them.

03 **App Config** – This can be used to store common application configurations.

AWS Systems Manager

01 **Change Manager** – You can manage the changes within your organization when it comes to application and infrastructure changes.

02 **Automation**– You can automate common maintenance and deployment tasks.

03 **Inventory** – This service creates a software inventory of the softwares running on your managed nodes.

AWS Systems Manager

01 **Patch Manager** – This allows you to automate the release of patches on your nodes such as your EC2 Instances.

02 **State Manager** – This ensures that your nodes are in a defined state.

03 **Incident Manager** – This can be used to manage incidents that affect AWS resources.

AWS
Systems Manager

AWS Systems Manager – Parameter Store

01 Here you can store your configuration data and secrets.

02 You can store information such as database passwords, license code. All of these are stored as parameter values.

03 You can then reference these parameters in your scripts , commands etc.

AWS
Credential report

AWS Credential report

01 You can use this feature to generate and download a credential report.

02 This report contains the list of users and their status.

03 You can use this when it comes to compliance.

AWS MFA

MFA in AWS

01 The use of MFA - Multi-Factor Authentication to provide an extra layer of security when it comes to authentication.

02 It's a good practice to enable MFA for your privileged users.

03 There are different authentication mechanisms available.

MFA in AWS

01 Virtual MFA devices - This is a software that runs on a phone or another device.

02 Hardware MFA device - This generates a numeric code that the user can use to log into the account.

03 FIDO security key - This isa device that can plug into your computer that can be used in the authentication process.

Amazon GuardDuty

Amazon GuardDuty

01 This is a service that can be used to detect any sort of malicious activity occurring from within your AWS account.

02 It can do this by analyzing the data within various data sources such as AWS CloudTrail, Amazon S3 logs, DNS logs etc.

03 It uses threat intelligence feeds, known IP addresses, machine learning to understand these different sort of threats.

Amazon GuardDuty

01 You can also enable a separate Malware Protection feature when it comes to Amazon EBS volumes.

02 This service is a regional service.

03 If any potential security issue is discovered , it comes up as a finding.

Amazon Cognito

Amazon Cognito

01 This service is used to provide authentication,authorization and user management for web and mobile applications.

02 Here you can define users. Users can sign in via a password.

03 Or they can sign in using third party credentials like Facebook or Google.

Amazon Cognito

01 User pools – These are user directories that provide the sign-up and sign-in option for users.

02 Identity pools – These helps to grant access to users to AWS services.

Domain – Cloud Concepts

AWS Well-Architected Framework

Operational Excellence

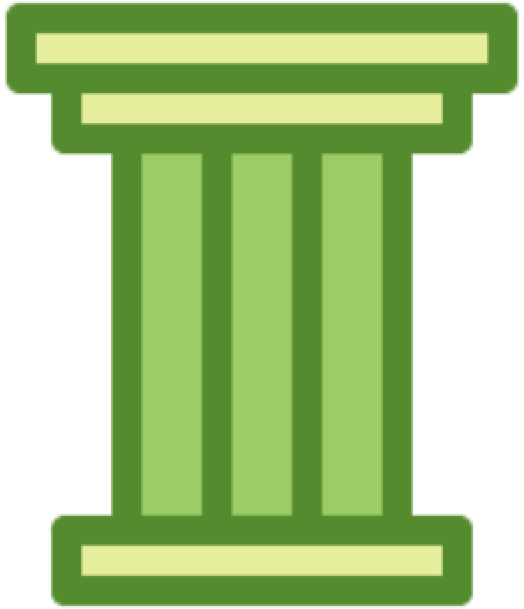
Includes the ability to support development and run workloads effectively, gain insight into their operations, and to continuously improve supporting processes and procedures to deliver business value.

Security

Encompasses the ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security.

Reliability

Encompasses the ability of a workload to perform its intended function correctly and consistently when it’s expected to. This includes the ability to operate and test the workload through its total lifecycle.

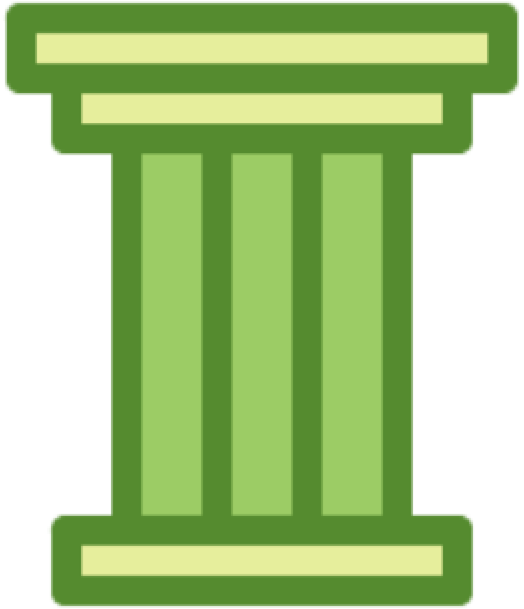


Performance **Efficiency**

Includes the ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.

Cost
Optimization

Includes the ability to run systems to deliver business value at the lowest price point.



Sustainability

Focuses on environmental impacts, especially energy consumption and efficiency, since they are important levers for architects to inform direct action to reduce resource usage.

Domain – Billing and Pricing

Domain – Cloud Concepts

Consolidated Billing

Consolidated Billing

01 You can use this feature to consolidate the bill from multiple AWS accounts.

02 The management account can pay the bills for the member accounts.

03 Here you need to setup an AWS Organization.

Consolidated Billing

01 Benefit – You get one consolidated bill.

02 There is no additional cost to use this feature.

03 When you have combined usage across accounts, there are volume discount pricings that you can avail.

AWS Expenditure

AWS Expenditure

01 Capital Expenditure , Capital Expense or CAPEX.

02 Here the organization spends money to buy an asset.

03 Or it just spends money to improve a fixed asset.

AWS Expenditure

01 For example – Buying server racks and servers for a data center.

02 The company is making an investment.

03 When it comes to the AWS Cloud, you don’t have to make this investment.

AWS Expenditure

01 Operational Expenditure , OPEX

02 Here the organization spends money on an on-going basis.

03 Personnel to maintain a data center.

AWS Expenditure

01 With AWS , most of the expenses can come under the aspect of operational expenses.

02 The on-going cost of running an EC2 Instance.

03 The on-going cost of storing objects in an S3 bucket.

AWS
Budgets

AWS Budgets

01 This can be used to track your AWS cost and usage.

02 You can also take appropriate action based on the cost and usage.

03 You can setup a monthly cost budget.

AWS Budgets

01 You can create cost budgets, usage budgets, RI utilization and Saving plans budgets.

02 You can setup AWS Budget actions.

03 You can setup AWS Budget notifications.

AWS
Cost Explorer

AWS Cost Explorer

01 Here you can view and analyze your costs.

02 Via the Cost Explorer Interface you can view the costs for free.

03 Programmatic calls to the Cost Explorer have a charge.

AWS Cost Explorer

01 You can view data for the last 12 months.

02 It also helps you to forecast how much you are likely to spend for the next 12 months.

03 You can also get recommendations on what Reserved Instances to purchase.

AWS

Cost and Usage Reports

AWS Cost and Usage Reports

01 Here you can get your complete cost and usage reports.

02 You can also publish the billing reports to an Amazon S3 bucket.

03 You can receive the costs per hour, day or by month.

Resource Tagging

Resource Tagging

01 You can actually assign metadata to your AWS resources.

02 This is done in the form of tags.

03 A tag is nothing but a key-value pair.

Resource Tagging

01 **Use case** – Organize resources department-wise

02 **Use case** – Cost allocation department-wise. You can actually use AWS Cost Explorer to see the cost of resources tag wise.

03 **Use case** – IAM Policies also support tag-based conditions